

A BILL FOR AN ACT TO PROVIDE FOR THE ESTABLISHMENT OF THE DATA PROTECTION COMMISSION CHARGED WITH THE RESPONSIBILITY FOR THE PROTECTION OF PERSONAL DATA AND DATA SUBJECTS' RIGHTS AND THE REGULATION OF THE PROCESSING OF PERSONAL INFORMATION; AND FOR RELATED MATTERS (HB. 02)

Provisions of the Bill	Committee of the Whole Recommendations
Part I - Objectives, Application And Scope Objectives of the Bill 1.-(1) The primary objective of this Bill is to provide an efficient regulatory framework for the protection of Personal Data and to regulate the processing of information relating to Data Subjects and to safeguard their fundamental rights and freedoms as guaranteed under the Constitution, as amended. Specifically, the Bill seeks to achieve the following- (a) promote a code of practice that would ensure the privacy and protection of Data Subject data without unduly undermining the legitimate interests of commercial organizations and government security agencies for such personal data; (b) minimize the deleterious effect of personal data misuse or abuse on data subjects and other victims; (c) establish an impartial, independent and effective regulatory authority that will coordinate and superintend over Data Protection and Privacy of Data Subject data held by Data Controllers and Data Processors within the private and public Sectors; (d) to ensure that the processing of personal data is processed in a transparent, fair, and lawful manner, on the basis of Data Subject consent or in accordance with the data protection principles stipulated in this Bill or other legislation.	Retained
Application and Scope 2.(1) The Bill applies to the processing and use of personal data relating to individuals by automated and non-automated means, irrespective of their nationality or residence and in particular by- (a) requiring that Personal Data is processed in a transparent, fair and lawful manner, on the basis of an individual's consent or another specified lawful basis; (b) conferring on individuals a number of rights as set in Part V, including the right to be informed about the processing of their Personal Data, to obtain a copy of such data, the right to the rectification of inaccurate data and the right to remedy. (2) The Bill applies to personal data processed by entities in the private and public sectors throughout the Federal Republic of Nigeria. (3) This Bill does not apply to processing of personal data carried out by a Data Subject in the course of a purely personal or household activity. (4) Except as otherwise provided, this Bill applies to a Data Controller and Data Processor in respect of Personal Data where- (a) the Data Controller and Data Processor is established in Nigeria and the Personal Data of Data Subjects in Nigeria are processed within the territory of Nigeria, (b) the Data Controller is not established in Nigeria but uses equipment or a Data Processor in Nigeria to process Personal Data of Data Subjects who are within the territory of Nigeria, or (c) processing is carried out in respect of information relating to Data Subjects who are within the territory of Nigeria and Personal Data which originates partly	Retained

or wholly from Nigeria. (5) For the purposes of this Bill, the following are to be treated as established in Nigeria: (a) a Data Subject who is ordinarily resident in Nigeria; (b) a body incorporated under the laws of Nigeria; (c) a partnership, persons registered under the relevant laws of the Nigeria; (d) an unincorporated joint venture or association operating in part or in whole in Nigeria; and (e) any person who does not fall within paragraphs (a),(b), (c) or (d) above, but maintains an office, branch or agency through which business activities are carried out in Nigeria. (6) A Data Controller and Data Processor who is not incorporated in Nigeria shall register with the Commission if the Data Controller or Data Processor, processes data of Data Subjects within the territory of Nigeria. (7) The categories of data to which this Bill applies includes- (a) Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership; (b) genetic data; (c) personal banking and accounting recording including biometric data for the purpose of uniquely identifying a natural person; (d) data concerning health; (e) data concerning a natural person's sex life; (f) Personal Data relating to criminal offences, including criminal records; (g) Personal data revealing an Data Subject's flight reservation/itinerary; (h) Student's education records; (i) Personal medical and health records; (j) Telephone calls , call data records, messages, websites visited by mobile phone, personal videos, pictures and other information stored on the mobile phone; (k) Cable TV subscriber data and viewership pattern to reveal Data Subject behavior; (l) Video rental records whether procured and stored digitally or in any other form; and (m) Such other categories of data usually processed by service providers, commercial entities as may be determined by the Guidelines of the Commission to be protected under this Bill.	
<u>Part II - Basic Principles And Legal Basis For Processing Of Personal Data</u> Basic Principles relating to Processing of Personal Data 3.-(1) Personal Data shall be- (a) processed lawfully, fairly and in a transparent manner and shall be proportionate in relation to the legitimate purpose pursued and reflect at all stages of the processing a fair balance between all interests concerned, whether public or private, and the rights and Data Subject freedoms protected by law; (b) collected for specified, explicit and legitimate purposes. Personal Data should not be further processed for a purpose that is Incompatible with those purposes for which the data were initially collected. Further processing for archiving purposes in the public interest, for scientific purposes or historical research purposes and statistical purposes in accordance with any relevant law in Nigeria shall not be considered to be incompatible with the initial purposes; (c) adequate, relevant and limited to what is necessary in relation to the	Retained

purposes for which they are processed; (d) be accurate and regularly kept up to date; (e) kept in a form that permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data are processed. Data should be deleted once the purpose for which they were processed has been achieved or should be kept in a form that prevents any direct or indirect identification of the Data Subject; (f) processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorized or unlawful processing and access, against loss, destruction or damage. The Data Controller and Data Processor shall use appropriate technical and organizational measures to ensure the integrity and the confidentiality of the Personal Data.	
Lawfulness of Personal Data Processing 4.-(1) The processing of Personal Data shall be carried out on the basis of the free; specific; informed and unambiguous consent of the Data Subject or principles and legal basis stipulated in this Bill. (2) From the commencement of this Bill, any of the following shall constitute lawful basis for processing of personal data- (a) processing is necessary for the performance of a contract to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract; (b) processing is necessary for compliance with a legal obligation as provided by law and to which the Data Controller is subject; (c) processing is necessary in order to protect the vital interests of the Data Subject or of another natural person; (d) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller; (e) processing is necessary for the purposes of the prevailing legitimate interests pursued by the Data Controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject, in particular where the Data Subject is a child.	Retained
Consent of Data Subjects 5.-(1) Where processing of personal data is based on consent, the Data Controller shall be able to demonstrate that the Data Subject has consented to the processing of his Personal Data. (2) The consent of the Data Subject shall represent the free expression of an intentional choice given by a statement (either in writing or orally) or by a clear affirmative action. (3) Mere silence, inactivity or pre-validated forms or boxes shall not constitute consent by the Data Subject. (4) Where the Data Subject has no genuine choice or is unable to refuse consent, consent given under such circumstances shall not be regarded as valid consent. (5) Where the processing of Personal Data is based on the consent of the Data Subject, he shall have the right to withdraw his consent at any time. (6) The withdrawal of consent under subsection (5) of this section shall not affect the lawfulness of the data processing that occurred before the Data Controller has received the notification for withdrawal of consent.	Retained

Transparency of Personal Data Processing 6.-(1) Every Data Subjects has the right to be informed ('to know') about the processing of their Personal Data and their rights. (2)A Data Controller shall act transparently when processing Personal Data in order to ensure fair processing and to enable Data Subjects to understand and exercise their rights with regards to the processing of their personal. (3) A Data Controller shall inform the Data Subject of- (a) the Data Controller's official identity and habitual residence or place of establishment; (b) the contact details of the Data Controller, of the Data Protection Officer and, where applicable, the Data Controller's representative; (c) the legal basis and the purposes of the intended processing; (d) the categories of Personal Data processed; (e) the recipients or categories of recipients of the Personal Data; (f) any intended transfer of Personal Data to a third party or foreign nation or international organization and a description of the safeguards provided to ensure the adequate protection of Personal Data; (g) the period for which Personal Data will be retained or if that is not possible, the general criteria used to determine that period; (h) the existence of automated decision-making, including profiling together with the significance and envisaged consequence of such processing for the Data Subject, including the right to object and challenge such processing; (i) the existence of profiling and the consequences of such profiling and the right to object; (j) the existence of rights set out in Part III of this Bill including the right to lodge a complaint with the Data Protection Commission and the means for exercising those rights; (k) Where processing is based on consent, the Data Subject shall be informed of the rights to withdraw his consent at any time. (4) The information referred to in subsection (3) of this section shall be provided in an appropriate format adapted to the relevant Data Subjects and shall be presented in a concise, transparent, intelligible and easily accessible form, using clear plain language. (5) The provision of subsection (3) of this section shall not apply where the Data Subject already received the information. (6) Where the Personal Data are not collected directly from the Data Subject, the Data Controller shall provide the information in subsection (3) of this section within a reasonable period but at the latest within one month or on first communication with the Data Subject, except where the processing is expressly prescribed by the provisions of this Bill or other legislation.	Retained
Part III - Establishment, Composition, Powers and Functions of the Data Protection Commission Establishment of the Data Protection Commission 7.-(1) There is established a Commission to be known as the Data Protection Commission (in this Bill referred to as the Commission) which shall be charged with the responsibility of regulating the processing of personal data and disclosure of Data Subject information and perform such other duties incidental	Retained

to the functions prescribed by this Bill. (2) The Commission shall be a body corporate with perpetual succession and a common seal and shall have the power to sue and be sued in its corporate name and, may hold, acquire and dispose of any property, movable or immovable. (3) The Commission may be structured into departments as the Commission may from time to time deem appropriate for the effective discharge of its functions under this Bill. (4) The Corporate Headquarters of the Commission shall be located in Abuja, the Federal Capital Territory of Nigeria with six zonal offices in the six geopolitical zones of Nigeria and State offices in any part of Nigeria as the Commission may designate.	
Composition of the Commission 8.-(1) The Commission shall consist of- (a) a full-time Data Protection Commissioner to be appointed by the President on the recommendation of the Attorney-General; (b) one member not below the Directorate cadre from the following: (i) Federal Ministry of Justice. (ii) National Identity Management Commission (iii) Nigerian Communication Commission (iv) National Information Technology Development Agency. (v) Nigerian Immigration Service (vi) Independent National Electoral Commission; (vii) National Population Commission; (c) One representative nominated by Data Controllers (d) One representative nominated by Data Processors (e) One representative nominated by civil society; and (f) The Secretary to the Commission, (2) The Data Protection Commissioner shall be paid salary and allowances payable in the public service while the part-time members shall be paid such emoluments, allowances and incidental expenses as the National Salaries, Incomes and Wages Commission may from time to time approve. (3) the supplementary provisions contained in the Schedule to this Bill shall have effect with respect to the tenure of members of the Commission and the proceedings of the Commission and other matters mentioned therein.	Retained
Functions of the Commission 9.-(1) The Commission shall- (a) Protect the personal data and privacy of Data Subject by regulating the processing of personal information; (b) provide the process to obtain, hold, use or disclose personal information; (c) ensure that Data Controllers and Data Processors adhere to the Data Protection principles as provided for by this Bill in order to protect the fundamental rights and freedoms, particularly privacy of natural persons in relation to the processing of their Personal Data; (d) assist the facilitation of the free flow of Personal Data through consultation and cooperation with other relevant agencies in compliance with established data security best practices; (e) act as supervisory authority, exercise investigative, corrective, regulatory, authorization and advisory powers. To this end, the Commission shall-	Retained

(i) Give advice and approve high risk processing operations and systems of Data Controllers and Data Processors in order to ensure compliance of their processing operations with the provisions of this Act; (ii) Issue warnings to a Data Controller or Data Processor in the event that intended processing operations are likely to infringe the provisions of this Act; (iii) receive and process claims from Data Subjects whose rights have been infringed; (iv) order the rectification, completion or deletion of Personal Data and impose a temporary or definitive limitation, including a ban, on processing operations; (v) receive information concerning data breaches from Data Controllers and Data Processors, investigate such breaches and communicate those breaches to the Data Subjects and the public, where provided for by law; (vi) impose administrative fines or sanctions where Data Controllers and Data Processors infringe any provision of this Act and where the infringement is of an intentional or negligent character; and (vii) have the power to engage in legal proceedings or to bring to the attention of the competent judicial authorities or law enforcement agencies violations of the provisions of this Act. (f) The Commission shall act with complete independence and impartiality in performing its duties and exercising its powers and in doing so shall neither seek nor accept instructions; (g) The Commission shall promote public awareness of the rights of Data Subjects and the exercise of their rights. It shall inform Data Controllers and Data Processors of their duties and responsibilities and shall share best practices in order to ensure the free flow of Personal Data; (h) The Commission shall be consulted on proposals for any legislative or administrative measures which relate to the processing of Personal Data; (i) The Commission shall provide relevant Regulations, Guidelines, and Policies relating to transfers of Personal Data provided for under this Act, or any other legislation. (j) The Commission shall muster the resources necessary for the effective performance of its functions and the exercise of its powers; (k) The Commission shall prepare and publish its reports biannually, outlining its activities which shall be submitted to the President.	
Powers of the Commission 10.-(1) To carry out its functions, the Commission shall have power to- (a) Implement and monitor compliance with the provisions of this Act; (b) make the administrative arrangements it considers appropriate for the discharge of its duties; (c) investigate any complaint under this Act and determine it in the manner the Commission considers fair; (d) powers to impose fines and penalties to enforce compliance and redress. (e) make such regulations as may be necessary or expedient for carrying out its functions and enforcing the provisions of this Act and do all such things as are necessary for or incidental to the carrying out of its functions and duties under this Bill; (f) Apply to the appropriate court for the issuance of such warrant relevant for the performance of its functions under this Act.	Retained
Part IV - The Data Protection Commissioner and other Staff of the Commission Appointment of Data Protection Commissioner/Chief Executive Officer 11.-(1) There shall be for the Commission, a Data Protection Commissioner, who shall -	Retained

(a) be appointed by the President on the recommendation of the Attorney - General of the Federation and Minister of Justice; (b) be the Chief Executive Officer and Accounting Officer of the Commission and be responsible for- (i) the day to day administration of the Commission; (ii) the execution of the policies and decisions of the Commission; (iii) performance of such other functions as may be necessary or incidental for the due execution of the mandate of the Commission. (c) hold office in the first instance for a term of five years and may be reappointed for another term of five years and no more; (d) not be qualified for appointment as a Data Protection Commissioner unless they possess professional skills and at least 15 years of cognate experience in these fields: law, Data Protection Policy, Cybersecurity Management, Information Communication Technology, or Management Science.	
Cessation or Removal from office. 12.-(1) notwithstanding the provisions of section 1 of this Act and where the Data Protection Commissioner resigns his appointment by a notice in writing under his hand addressed to the President, the Data Protection Commissioner shall only be removed from office by a two third majority resolution of the Senate- (a) for inability to discharge the functions of his office (whether arising from infirmity of mind or body or any other cause) or for misconduct; (b) where it is established that it is not in the interest of the Commission or the public for him to continue in the office.	Retained
Secretary to the Commission 13.-(1) The Commission shall have a Secretary, who shall also be the Director Legal Services, appointed by the President based on the recommendation of the Attorney General of the Federation.	Retained
Staff of the Commission 14.-(1) The Commission shall have powers to appoint such number of other staff as it deems necessary for the proper and effective performance of its functions as staff of the Commission. (2) The employment of the Commission's staff shall be subject to such terms and conditions as may from time to time be stipulated by the Commission and contained in the respective staff's employment contracts.	Retained
Terms and Conditions of Service 15.-(1) The terms and conditions of service and remuneration of employees of the Commissions shall be determined in line with the appropriate authorities	Retained
Removal Discipline of Staff 16.- The removal and discipline of staff shall be in accordance with existing Public Service Rules and Regulations	Retained
Part V - Rights Of The Data Subjects Rights of Data Subjects 17.-(1) A Data Subject shall have the rights set out in this Part. (2) A Data Subject's rights may only be limited in accordance with the provisions of section 38 of this Act;	Retained
Right of Access 18.-(1) A Data Subject shall have the right: (a) to obtain, on request and at reasonable intervals and without excessive delay or expense, confirmation as to whether Personal Data relating to the Data Subject are being processed and if so, the communication in an intelligible form of the data, together with all available information on the origin of the Data, on	Retained

the preservation period as well as any other information that the Data Controller is required to provide in order to ensure the transparency of processing in accordance with section 6 of this Act; (b) to obtain, on request, knowledge of the reasoning underlying data processing where the results of such processing are applied to the Data Subject. (2) The Data Controller shall, free of charge, provide a copy of the Personal Data processed, and in exceptional circumstances, the Data Controller may charge a reasonable fee based on administrative costs where a request is excessive or manifestly unfounded, in particular because of their repetitive character, where the Data Controller demonstrates that it is not in a position to identify the Data Subject or as may be provided in a law- (a) The Data Controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request; (b) where the Data Controller has reasonable doubts concerning the identity of the Data Subject making the request, the Data Controller may request for the provision of additional information necessary to confirm the identity of the Data Subject. (3) The Data Controller shall provide a copy of the Personal Data requested together with the information under subsection (1) of this section within a period one month from the date of receipt of the request. (4) The period stated in subsection (3) of this section, may be extended by a period not exceeding an additional two months where necessary, taking into account the complexity of the request. (5) A Data Subject shall also have the right, on request, to obtain knowledge of the reasoning underlying data processing where the result of such processing is applied to him, including the consequence of such reasoning.	
Right in respect of Automated Decision Making 19.-(1) A Data Subject shall have the right not to be subject to a decision significantly affecting him based solely on an automated processing of data without having his view taken into consideration. (2) Subsection (1) of this shall not apply where a decision is authorized by law to which the Data Controller is subject and that provides appropriate measures to safeguard the legitimate interests, rights and freedoms of a Data Subject. (3) The Data Controller shall implement suitable measures to safeguard the Data Subject's rights and legitimate interests, at least the right to obtain human intervention on the part of the Data Controller.	Retained
Right to rectification, erasure, and restitution of processing 20.-(1) The Data Subject shall have the right to obtain from the Data Controller, without delay, free of charge, the rectification, blockage, or erasure of inaccurate, false or unlawfully processed Personal Data. (2) Where the Data Subject has submitted a valid request for the rectification or erasure of the Data Subject Personal Data, the Data Controller shall communicate such request to all Data Controllers, Data Processors or other recipients in order to ensure complete rectification or erasure.	Retained

(3) Where the accuracy of the data is contested by the Data Subject, the Data Subject opposes the erasure of his or her Personal Data, or the Data Subject has objected the processing of his or her Personal Data and the legal basis must be verified, the Data Controller shall temporarily block processing until the grounds for restriction have been resolved. Where the temporary blocking of Personal Data is lifted, the Data Subject shall be informed by the Data Controller.	
Right to Judicial Remedy 21. Where a right of a Data Subject right under this Act is violated, the Data Subject shall have the right to a judicial remedy under this Act.	Retained
Right to Assistance by the Commission 22. A Data Subject has the right to benefit, whatever his nationality or residence, from the assistance of the Commission within the meaning of section 5, in exercising his or her rights under this Act	Retained
Right to Object, including profiling and direct marketing 23. A Data Subject shall have the right to object at any time, on grounds relating to his or her situation, to the processing of Personal Data concerning him or her, including profiling	Retained
Right to have Data Processing Suspended 24.-(1) A Data Controller shall no longer process the Personal Data unless the Data Controller demonstrates legitimate grounds for the processing and a legitimate interest which overrides the interest or rights and fundamental freedoms of the Data Subject. (2) Data Subjects shall have the right to object to the processing of their Personal Data for the purposes of direct marketing at any time and free of charge. (3) A Data Controller shall not provide, use, obtain, procure or provide information related to a Data Subject for the purposes of direct marketing without the prior written consent of the Data Subject. (4) Where a Data Subject makes an objection under this section, he or she shall be entitled to have the unconditional erasure, removal or suppression of the Personal Data covered by the objection. (5) Where the Commission is satisfied on a complaint by a person who has given notice under this section that the Data Controller has failed to comply with the notice, the Commission may order the Data Controller to comply with the notice. (6) In this section "direct marketing" includes the communication by whatever means of any advertising or marketing material which is directed to particular Data Subjects.	Retained
Right to prevent Processing of Personal Data 25.-(1) A Data Subject shall at any time by notice in writing to a Data Controller and Data Processor require, if the processing is not authorized by law or other valid legal ground the Data Controller and Data Processor to cease or not begin processing of Personal Data for a specified purpose or in a specified manner, data which causes or is likely to cause unwarranted damage or distress to the Data Subject. (2) A Data Controller and Data Processor shall within twenty-one days after receipt of a notice inform the Data Subject in writing-	Retained

(a) that the Data Controller or Data Processor has complied or intends to comply with the notice of the Data Subject, or; (b) of the reasons for non-compliance. (3) Where the Commission in accordance with this Act is satisfied that the complaint is justified, the Commission shall order the Data Controller or Data Processor to comply with the notice submitted pursuant to subsection (1).	
Right to Data Portability 26.-(1) A Data Subject shall have the right to receive the Personal Data concerning him or her which was provided to a Data Controller, in a structured, commonly used and machine -readable format and have the right to transmit those data to another Data Controller without hindrance from the Data Controller from where the Personal Data is withdrawn provided - (a) the processing is based on consent or on a contract; (b) the processing is carried out by automated means (2) In exercising his or her right to data portability pursuant to subsection (1) of this section, the Data Subject shall have the right to have his or her personal data transmitted directly from one Data Controller to another where technically feasible. (3) The exercise of the right referred to in subsection (1) of this section shall not Apply to data processing necessary for the performance of the task carried out in the public interest or in the exercise of official authority vested in the Data Controller, and the right shall not adversely affect the rights and freedoms of others.	Retained
Part VI - Processing of Sensitive Data Processing of Sensitive Data 27.-(1) Unless otherwise provided by this Act or other legislation, a person shall not process Personal Data which relates to- (a) a child who is under parental control in accordance with the law, or (b) the religious or philosophical beliefs, ethnic origin, race, trade union membership, political opinions, health, sexual life or behavior of a Data Subject. (2) A Data Processor or Data Controller may process Sensitive Personal Data in accordance with this Act where- (a) processing is necessary as provided under this Bill; or (b) the Data Subject consents or in the case of a child under parental control, the prior consent of the parent or Guardian is obtained before processing. (3) The processing of Sensitive Data is necessary where it is for the exercise or performance of a right or an obligation conferred or imposed by law on an employer. (4) Personal Data shall not be processed unless the processing is necessary for the protection of the vital interests of the Data Subject where- (a) it is impossible for consent to be given by or on behalf of the Data Subject,	Retained

(b) the Data Processor or Data Controller cannot reasonably be expected to obtain the consent of the Data Subject, or (c) consent by or on behalf of the Data Subject has been unreasonably withheld. (d) where it is impossible or impracticable to obtain to obtain the consent of the data subject , the Data Processor or Data Controller shall depose to an affidavit to the effect that it is impracticable to obtain the requisite consent and necessary to carry out the processing of the sensitive data in accordance with the provisions of this section. (5) Sensitive data shall not be processed unless the processing is carried out for the protection of the legitimate activities of a body or association which- (a) is established for non-profit purposes, (b) exists for political, philosophical, religious or trade union purposes; (c) relates to Data Subjects who are members of the body or association or have regular contact with the body or association in connection with its purposes, and (d) does not involve disclosure of the Personal Data to a third party without the consent of the Data Subject. (6) The processing of sensitive data shall be presumed to be necessary where it is required- (a) for the purpose of or in connection with a legal proceeding, (b) to obtain legal advice, (c) for the establishment, exercise or defence of legal rights, (d) in the course of the administration of justice, or. (e) for medical purposes and the processing is- (i) undertaken by a health professional, and (ii) pursuant to a duty of confidentiality between patient and health professional. (7) In this section, "medical purposes" includes the purposes of preventive medicine, medical diagnosis, medical research, provision of care and treatment and the management of healthcare services by a medical or dental practitioner or a legally recognized traditional healer recognized by legislation regulating traditional medicine practice. (8) A person shall not process Sensitive Data in respect of race or ethnic origin unless the processing of the sensitive data is- (a) necessary for the identification and elimination of discriminatory practices, and (b) carried out with appropriate safeguards for the rights and freedoms of the Data Subject. (9) The Commission may by Notice, Guidelines or Regulations prescribe further conditions to be taken into consideration by the Data Processor and Data Controller for the maintenance of appropriate safeguards for the rights and freedoms of a Data Subject related to processing of sensitive Personal Data.	
Prohibition on Processing of Sensitive Data which relates to religious beliefs 28.-(1) The prohibition on processing of Personal Data which relates to the religious or philosophical beliefs of a Data Subject does not apply if the processing is carried out by- (a) a spiritual or religious organization or a branch of the organization and the processing is in respect of persons who are members of the organization,	Retained

(b) an institution founded on religious or philosophical principles and the processing is- (i) with respect to the members, employees or other persons belonging to the institution, (ii) consistent with the objects of the institution, and (iii) necessary to achieve the aims and principles of the institution. (2) A Data Subject who believes that their personal data is being processed under subsection (1) may at any time by notice in writing to a Data Controller require a Data Processor or Data Controller to provide particulars of data processed under this exemption.	
Rights in Relation to automated decision making 29.-(1) A Data Subject shall not be subjected to a decision significantly affecting him or her based solely on an automated processing of data, in violation of his rights under this Bill. (2) A Data Subject is entitled at any time by notice in writing to Data Controller to require the Data Controller to ensure that any decision taken by or on behalf of the Data Controller which significantly affects that Data Subject is not based solely on the processing by automatic means of Personal Data in respect of the Data Subject. (3) In the absence of a notice, where a decision which significantly affects a data subject is based solely on automated processing- (a) the Data Controller shall as soon as reasonably practicable notify the Data Subject that the decision was taken on that basis, and (b) the Data Subject is entitled, by notice in writing to require the Data Controller to reconsider the decision within twenty-one days after receipt of the notification from the Data Controller. (4) The Data Controller shall within twenty-one days after receipt of the notice, inform the Data Subject in writing of the steps that the Data Controller intends to take to comply with the notice. (4) This section does not apply to a decision made- (a) in the course of considering whether to enter into a contract with the Data Subject, (b) with a view to entering into the contract, (c) in the course of the performance of the contract, (d) for a purpose authorized or required by or under an enactment, (e) In other circumstances prescribed by the Commission. (5) where a data subject under this section is not satisfied with the response of the Data Controller, the Data Subject may file a complaint against the Data Controller to the Commission. (6) Where the Commission is satisfied on a complaint by a Data Subject that a person taking a decision has failed to comply, the Commission may order the Data Controller to comply. (7) An order for compliance under subsection (6) of this section shall not affect	Retained.

the rights of a person other than the Data Subject or the Data Controller	
Compensation for failure to comply 30.-(1) Where a Data Subject suffers damage through the contravention by a Data Controller or Data Processor of the requirements of this Bill, he is entitled to compensation from the Data Controller or Data Processor for the damages as may be determined by the court. (2) In proceedings against a Data Controller or Data Processor under this section, it is a defense to prove that the Data Controller or Data Processor took reasonable care in all the circumstances to comply with the requirements of this Bill	Retained
Part VII - Duties of Data Controllers and Data Processors Duties of Data Controllers 31.-(1) The Data Controller shall- (a) take all necessary technical and organizational measures to comply with, and be able to demonstrate, in particular to the Data Protection Commission, that the processing of Personal Data is performed in accordance with this Bill; (b) take all necessary measures to comply with the obligations of this Act; (c) ensure the processing of Personal Data is proportionate, that is, necessary in relation to the legitimate purpose pursued and having regard to the interests, rights and freedoms of the Data Subject or the public interest; (d) take into consideration the risks arising from the interests, rights and fundamental freedoms of Data Subjects, according to the nature and volume of the data, the nature, scope and purpose of the processing and, where appropriate, the size of the Data Controller or Data Processor; (e) be able to establish, in particular, to the data protection supervisory authority, that the processing under their control is in compliance with the provisions of this Act; (f) where applicable, appoint a Data Protection officer responsible for compliance with the obligations under this Act, take reasonable efforts to put in place appropriate data protection safeguards, policies, standards, procedures and security measures in accordance with the provisions of this Act. (2) For the purpose of this section, each Ministry, Department and Agency of the Federal government shall be treated as a Data Controller. (3) Each department shall designate an officer to act as a data supervisor. (4) Where the purposes and the manner in which the processing of Personal Data are determined by a person acting on behalf of the Executive, Legislature and the Judiciary, the Data Controller in respect of that data for the purposes of this Bill is- (a) in relation to the Executive, the relevant permanent secretary or Director, (b) in relation to Parliament, the Clerk to National Assembly or Clerk to House of Assembly of a State, and (c) in relation to the Judiciary, the Secretary, National Judicial Council or relevant chief registrar.	Retained

(5) A different person may be appointed under subsection (4) for a different purpose	
Data Breach Notification 32.-(1) In the case of a data breach and risks to the rights and freedoms of natural persons, the Data Controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the Commission of the data breach. (2) Where the notification to the commission is not made within 72 hours, it shall be accompanied by reasons for the delay; (3) The Data Processor shall notify the Data Controller without undue delay after becoming aware of a personal data breach. (4) The notification referred to in subsection 1 of this section shall at least- (a) describe the nature of the Personal Data breach including where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of personal data records concerned; (b) communicate the name and contact details of the Data Protection Officer or other contact point where more information can be obtained; (c) describe the likely consequences of the Personal Data breach; (d) describe the measures taken or proposed to be taken by the Data Controller to address the Personal Data breach, including, where appropriate, measures to mitigate its possible adverse effects. (5) Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay. (6) The Data Controller shall document any Personal Data breaches, comprising the facts relating to the Personal Data breach, its effects and the remedial action taken. The documentation shall enable the Commission to verify compliance with this Act. (7) Data Controller shall notify the Data Subject of a breach- (a) When the Data breach is likely to result in a high risk to the rights and freedoms of natural persons, the Data Controller shall communicate the Data breach to the Data Subject without undue delay; (b) The communication to the Data Subject referred to in subsection 7 (a) shall describe in clear and plain language the nature of the Personal Data breach. (c) The communication to the Data Subject referred to in subsection 7 (a) shall not be required if any of the following conditions are met- (i) the Data Controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the Personal Data affected by the Personal Data breach, in particular those that render the Personal Data unintelligible to any person who is not authorized to access it, such as encryption; (ii) the Data Controller has taken subsequent measures which ensure	Retained

(iii) that the high risk to the rights and freedoms of data subjects referred to in subsection 7(a) is no longer likely to materialise; it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner. (d) If the Data Controller has not already communicated the personal data breach to the data subject, the commission, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in Sub-section (7 (c) are met.	
Liability of Data Processors 33.-(1) The Data Controller shall be responsible for the processing of Personal Data carried out on behalf of the Data Controller. (2) The Data Controller shall use only a Data Processor who provides sufficient guarantees to implement appropriate technical and organizational measures, taking into account the Data Controller's obligations under this Bill and ensure the protection of the rights and fundamental freedoms of the Data Subject (3) The processing of Personal Data by the Data Processor on behalf of the Data Controller shall be subject to a legally binding contract that sets-out the nature of the processing agreement, including the Personal Data to be processed and the purpose of processing, that stipulates the obligations and restrictions to be imposed on the Data Processor, including sub-processing or transfers of Personal Data to third countries.	Retained
Duties of Data Processors 34.-(1) A Data Processor shall: (a) Process Personal Data on behalf of a Data Controller only on documented instructions of the Data Controller; (b) not engage another Data Processor without the prior written authorization of the Data Controller; (c) A Data Processor shall inform the Data Controller of changes concerning the addition or replacement of Data Processors; (d) inform the Data Controller of any legal requirement that may create risks to the rights and fundamental freedoms of Data Subjects, unless the law prohibits such notice; (e) take appropriate technical and organizational security measures pursuant to section 37; (f) in so far that it is possible and not unreasonable, assist the Data Controller by putting in place the appropriate technical and organizational measures for the fulfillment of the Data Controller's obligations to respond to the rights pursuant to this Bill; (g) assist the Data Controller in ensuring compliance with its security obligations pursuant to Section 37 of this Bill, including security breach notification pursuant to section 32 of this Bill; (h) at the request of the Data Controller, delete or return all Personal Data to the Data Controller after the end of the provision of services, and delete any copies of Personal Data unless prohibited by law; (i) make available to the Data Controller all information necessary to assist the Data Controller demonstrate compliance with its obligations under this Bill and	Retained

allow and facilitate audits conducted by the Data Controller or a third-party auditor determined by the Data Controller; (2) Where a Data Processor engages another Data Processor to meet its obligations to the Data Controller, the Data Processor shall impose the same data protection obligations set in its contract with the Data Controller. The initial Data Processor shall be liable to the Data Controller for ensuring the performance of the other Data Processors obligations. (3) The Data Processor and any other party acting under the authority of the Data processor or Data Controller, and who has access to the Personal Data shall not process those data except on instructions from the Data Controller, and unless otherwise required by law. (4) The Data Processor, and where applicable the Data Processor's representative shall maintain a record of processing activities pursuant to this Bill.	
Part VIII - Data Protection by Design and Security of Processing Data Protection by Design (and by default) 35.-(1) The Data Controller and, where applicable, the Data Processor, shall- (a) examine the likely impact of the intended processing of Personal Data on the rights and fundamental freedoms of Data Subjects prior to the commencement of such processing, and (b) design the data processing in such a manner, and integrate appropriate technical and organizational measures, as to prevent or minimize the risk of interference with those rights and fundamental freedoms.	Retained
Data Localization 36. The Data Commissioner shall mandate Data Controllers and Data Processors of Personal Data pursuant to this Act, to record, systematize, accumulate, store, host, amend, update and retrieve Personal Data on devices that are physically located within Nigeria's territorial jurisdiction".	Retained
Security of Processing 37.-(1) The Data Controller, and where applicable, the Data Processor, shall take necessary technical and organizational measures to protect Personal Data against risks such as accidental or unauthorized access to, destruction, loss, use, modification or disclosure of Personal Data. (2) When considering necessary measures, the Data Controller shall take into account- (a) the current state of the art of data-security methods and techniques in the field of Data processing, commensurate with the seriousness and probability of the potential risk; (b) factors such as the- (i) potential adverse consequences for the Data Subject, (ii) nature of the Personal Data, (iii) volume of Personal Data processed, (3) Data Controllers and Data Processors shall establish a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.	Retained

Part IX - Exceptions, Restrictions and Exemptions Exception to the privacy of Personal Data. 38.-(1) No exception to the provisions set out in the this Bill shall be allowed except when such an exception is provided for by law and in recognition of the fundamental rights and freedoms of citizens and constitutes a necessary and proportionate measure in a democratic society. (2) The exception in order to be considered as necessary and proportionate in a democratic society has to be provided for by law, needs to serve a legitimate purpose as set out in the Constitution or an Act of the National Assembly and has to be proportionate to the legitimate aim pursued.	Retained
Exceptions on the grounds of Public Interest 39.-(1) The privacy of personal data is exempt from the provisions of this Bill for the purposes of- (a) public order, (b) public safety, (c) public morality, (d) national security, or (e) public interest. (2) (a) The privacy of Personal Data is exempt from the provisions of this Bill for the purposes of- (i) the prevention or detection of crime, (ii) the apprehension or prosecution of an offender, or (iii) the assessment or collection of a tax or duty or of an imposition of a similar nature. (3) Personal Data is exempt from the non-disclosure provisions in any case in which- (a) The disclosure is for a purpose mentioned in subsections (1) and (2) of this section; (b) the application of those provisions in relation to the disclosure is likely to prejudice any of the matters mentioned in that subsection. (4) Health, education and social work; Personal Data on the following subjects shall not be disclosed except where the disclosure is required by law- (a) Personal Data which relates to the physical, mental health or mental condition of the Data Subject, (b) Personal Data in respect of which the Data Controller is an educational institution and which relates to a pupil at the institution, or Personal Data of similar description. (5) The provisions of this Bill do not apply to the processing of Personal Data for protection of members of the public- (a) against loss or malpractice in the provision of- (i) banking, (ii) insurance, (iii) investment, (iv) other financial services, or	Retained

- (v) management of a body corporate;
- (b) against dishonesty or malpractice in the provision of professional services;
- (c) against the misconduct or mismanagement in the administration of a non-profit making entity;
- (d) to secure the health, safety and welfare of persons at work; or
- (e) to protect non-working persons against the risk to health or safety arising out of or in connection with the action of persons at work.

(6) A person shall not process Personal Data unless-

- (a) The processing is undertaken by a person for the publication of a literary or artistic material;
 - (b) the Data Controller reasonably believes that publication would be in the public interest; and
 - (c) the Data Controller reasonably believes that, in all the circumstances, compliance with the provision is incompatible with the special purposes:
- Provided that in the observance of these exemptions under this section, the Data Controller is not exempted from compliance with the data principles relating to;
- (a) lawful processing,
 - (b) data minimization,
 - (c) further processing,
 - (d) information quality, and
 - (e) Security safeguards.

(7) For the purposes of subsection (1) of this section , in considering whether the Data Controller believes that the publication would be in the public interest or is reasonable, regard may be had to the compliance by the Data Controller with any code of practice which is;

- (a) relevant to the publication in question, and
- (b) Designated by the Commission for purposes of this subsection.

(8) Further processing of personal Data for a research purpose is not to be regarded as incompatible with the purposes for which the data was obtained and for this reason-

- (a) Personal Data which is processed for research purposes in compliance with the relevant conditions may be kept indefinitely.
- (b) Personal Data which is processed only for research purposes is exempt from the provisions of this Bill if-
 - (i) the data is processed in compliance with the relevant conditions, and
 - (ii) the results of the research or resulting statistics are not made available in a form which identifies the Data Subject or any of them.
- (c) Personal Data is not to be treated as processed otherwise than for research purposes merely because the data is disclosed;
- (d) to any person for research purposes only,
- (e) to the Data Subject or a person acting on behalf of the Data Subject,
- (f) at the request or with the consent of the Data Subject or a person acting on behalf of the Data Subject ,or
- (g) in circumstances in which the person making the disclosure has reasonable grounds to believe that the disclosure falls within this section.

(9) Personal Data is exempt from the provisions on non-disclosure where the disclosure is required by or under an enactment, any rule of law or by the order of a court.

(10) Personal Data which is processed by a Data Subject only for the purpose of that Data Subject's personal, family or household purposes is exempt from the data protection principles. (11) Personal Data is exempt from the data protection principles if it consists of a reference given in confidence by the Data Controller for the purposes of - (a) education, training or employment of the Data Subject; (b) the appointment to an office of the Data Subject; or (d) the provision of any service by the Data Subject. (12) Personal Data is exempt from the subject information provisions where the application of the provisions is likely to prejudice the combat effectiveness of the Armed Forces of the Federal Republic of Nigeria. (13) The privacy of personal data is exempt from the provisions of this Bill if it needed to- (a) assess a person's suitability for judicial office, or (b) confer a national honour on the data subject. (14) The Commission may by legislative instrument make Regulations to prescribe exemptions from the subject information provisions of Personal Data processed to assess a person's suitability for- (a) employment by the government, or (b) any office to which appointments are made by the President. (15) Personal Data is exempt from the provisions of this Act if it relates to examination marks processed by a Data Controller- (a) to determine the results of an academic, professional or other examination or to enable the results of the examination to be determined, or (b) In consequence of the determination of the results. (16) Personal Data which consists of information recorded by candidates during an academic, professional or other examination is exempt from the provisions of this Act. (17) Personal Data is exempt from the subject information provisions if it consists of information in respect of which a claim to professional privilege or confidentiality between client and a professional adviser could be maintained in legal proceedings	
Part X - Administration and Enforcement Enforcement Notice 40.-(1) Where the Commission is satisfied that a Data Controller and Data Processor has contravened or is contravening any of the Data Protection principles stipulated under this Bill, the Commission shall serve the Data Controller with an enforcement notice to request that Data Controller to do any of the following- (a) to take or refrain from taking the steps specified within the time stated in the notice, (b) to refrain from processing any Personal Data or Personal Data of a description specified in the notice; or	Retained

(c) to refrain from processing Personal Data or Personal Data of a description specified in the notice for the purposes specified or in the manner specified after the time specified. (2) In deciding whether to serve an enforcement notice, the Commission shall consider whether the contravention has caused or is likely to cause damage or distress to any person. (3) An enforcement notice issued in respect of a contravention of a provision of this Bill may also require the Data Controller to rectify, block, erase or destroy other data held by the Data Controller and which contains an expression of opinion which appears to the Commission to be based on the inaccurate data. (4) Where- (a) an enforcement notice requires the Data Controller to rectify, block, erase or destroy Personal Data, or (b) the Commission is satisfied that Personal Data which has been rectified, blocked, erased or destroyed was processed in contravention of any of the data protection principles under this Bill, the Commission may require the Data Controller to notify a third party to whom the data has been disclosed of the rectification, blocking, erasure or destruction. (5) An enforcement notice shall contain a statement of the data protection principle which the Commission is satisfied has been contravened and the reasons for that conclusion. (6) Subject to the provisions of this section, an enforcement notice shall not require any of the provisions of the notice to be complied with before the end of the period stipulated in the Notice within which an appeal may be brought against the notice and, if the appeal is brought, the notice may not be complied with pending the determination or withdrawal of the appeal. (7) Notwithstanding the provisions of subsection (6) of this section, the Commission may in exceptional circumstances order that the notice apply immediately.	
Cancellation of Enforcement Notice 41.-(1) The Commission may on its own motion or on an application made by a person, on whom a notice is served, cancel or vary the notice to that person.	Retained
Request for Assessment 42.-(1) A person who is affected by the processing of any Personal Data may on that person's own behalf or on behalf of another person request the Commission to make an assessment as to whether the processing is in compliance with the provisions of this Act. (2) On receiving a request, the Commission may make an assessment in the manner that the Commission considers appropriate. (3) The Commission may consider the following in determining whether an assessment is appropriate: (a) the extent to which the request appears to the Commission to raise a matter of substance;	

(b) any undue delay in making the request; and (c) whether or not the person making the request is entitled to make an application in respect of the Personal Data in question. (4) The Commission shall not publish the report of any finding- (a) the request is accompanied with the prescribed fee, or (b) the Commission waives payment based on proven pecuniary challenges of the applicant. (5) Where the Commission finds that the processing by a Data Controller is contrary to the provisions of this Act, the Commission shall issue an information notice to the Data Controller specifying the contravention and give the Data Controller notice to cease processing Personal Data.	
Determination by the Commission 43.-(1) Where at any time it appears to the Commission that Personal Data (a) is being processed in a manner inconsistent with the provisions of this Act, or (b) is not being processed with a view to the publication by a person of a journalistic, literary or artistic material which has not previously been published by the Data Controller the Commission may make a determination in writing to that effect. (2) The Commission shall give a notice of the determination to the Data Controller	Retained
Restriction on Enforcement in case of processing for special purposes 44.-(1) The Commission shall not serve an enforcement notice on a Data Controller in relation to the processing of Personal Data under section 40 (1) (a) unless a determination has been made by the Commission.	Retained
Failure to Comply with Notice 45.-(1) A Data Controller or Data Processor who fails to comply with an enforcement notice or an information notice commits a breach and is liable to a fine as may be determined and imposed by the Commission. (2) It is a mitigating factor for a Data Controller or Data Processor under subsection (1) to prove that, that person exercised due diligence to comply with the notice in question.	Retained
Officer authorized by the Commission 46.-(1) The Commission may in writing authorize an officer to perform the functions determined by the Commission for the purpose of enforcing the provisions of this Act and the Regulations. (2) Without limiting subsection (1), an officer authorized by the Commission may at any reasonable time, enter to inspect and search any premises to ensure compliance with this Act.	Retained
Part XI - Trans-Border Flow of Personal Data Trans- border flow of personal Data 47.-(1) The transfer of Personal Data may only take place where an adequate level of protection based on the provisions of this Bill is secured in the recipient State or international organization. (2) An appropriate level of protection can be secured by- (a) the Data Protection laws of that State or international organization, including the applicable international treaties or agreements; or	Retained

(b) ad-hoc or approved standardized safeguards provided by legally-binding and enforceable instruments adopted and implemented by the Data Controllers or Data Processors involved in the transfer and further processing. (3) Notwithstanding the provisions of subsection (2) of this section the transfer of Personal Data may take place where- (a) the Data Subject has given explicit, specific and free consent, after being informed of risks arising in the absence of appropriate safeguards; (b) the specific interests of the Data Subject require it in the particular case; (c) prevailing legitimate interests, in particular important public interests, are provided for by law and such transfer constitutes a necessary and proportionate measure in a democratic society; or (d) it constitutes a necessary and proportionate measure in a democratic society for the freedom of expression. (4) The Commission shall be provided with all relevant information concerning the transfers of data referred to in subsection (1) of this section and, upon request, subsection (2) and (3) respectively, of this section. (5) The Commission is entitled to request that the person who carries out the data transfer demonstrates the effectiveness of the safeguards or the existence of prevailing legitimate interests. (6) The Commission may, in order to protect the rights and fundamental freedoms of Data Subjects, prohibit such transfers, suspend them or subject them to certain conditions. (7) The Commission shall ensure that where there is an onward transmission of Personal Data pursuant to this section, to any third party, other than the first recipient, such other party must meet the minimum requirement for transfer of Personal Data.	
Part XII - Offences and Penalties Unlawful obtaining of personal Data 48.-(1) A person commits an offence who knowingly or recklessly- (a) obtains or discloses Personal Data without the consent of the Data Controller or Data Subjects; (b) procures the disclosures of Personal Data to another person without the consent of the Data Controller or Data Subjects; or (c) after obtaining Personal Data, retains it without the consent of the person who was the Data Controller, and shall be liable on conviction to imprisonment for a term of not less than 3 years or to a fine of not less than N1,000,000.000:00 or to both such imprisonment term and fine. (2) It is a defence for a person charged with an offence under subsection (1) of this section to prove that the obtaining, disclosing, procuring or retaining of data- (a) was carried out for a legitimate purpose; for the purpose of this section, legitimate purpose will include preventing, detecting, prosecuting or investigating crime or any other legal purpose; (b) was required or authorized by an enactment, by a rule of law or by the order of a court or tribunal; (c) in the particular circumstances, was justified as being in the public interest; (d) was necessary for the purposes of national security in accordance with extant	Retained

legislation; (e) the person acted in the honest and reasonable belief that he had a legal right to obtain, disclose, procure or retain of the Personal Data; (3) A person commits an offence who sells Personal Data, where the person obtains the data in circumstances described under subsection (1) of this section, shall be liable on conviction to imprisonment for a term not less than 5 years or to a fine of not less than N3,000,000,000:00 or to both such imprisonment term and fine. (4) A person commits an offence who advertises or indicates that Personal Data where the person obtains the data in circumstances described under subsection (1) of this section, is or may be available for sale, shall be liable on conviction to imprisonment for a term not less than 5 years or to a fine of not less than N3,000,000,000.00 or to both such imprisonment term and fine.	
Failure to Localize Personal Data 49.-(1) A Data Controller or Data Processor commits an offence who fails to record, systematize, accumulate, store, host, amend, update and retrieve Personal Data on devices that are physically located within the country's territorial jurisdiction described under this Bill, and shall be liable on conviction to imprisonment for a term not less than 10 years or to a fine of not less than N8,000,000,000.00 or to both such imprisonment term and fine. (2) A Data Controller or Data Processor commits an offence who fails to put in place appropriate data protection safeguards, policies, standards, and procedures described under this Act shall be liable on conviction to imprisonment for a term not less than 8 years or to a fine of not less than N8,000,000,000.00 or to both such imprisonment term and fine.	Retained
Obstruction in the Execution of Warrant 50.-(1) A person commits an offence who- (a) intentionally obstructs an officer in the execution of a warrant issued under this Act, or fails without reasonable excuse to give the officer executing such a warrant such assistance as the officer may reasonably require for the execution of the warrant and shall be liable on conviction to imprisonment for a term not less than 2 years or to a fine of not less than N500,000,000.00 or to both such imprisonment term and fine. (2) A person who, in compliance with an information notice- (a) makes a statement which that person knows to be false in a material respect, or (b) recklessly makes a statement which is false in a material respect commits an offence and is liable on conviction to a fine not less than N10,000,000.00 or a term of imprisonment of not less than one year or to both.	Retained
Attempt, conspiracy, aiding and abetting 51.-(1) Any person who- (a) Attempts to commit any offence under this Bill; or (b) Aids, abets, conspires, counsel or procure another person(s) to commit any of the offences under this Bill: Commits an offence and shall be liable on conviction to the punishment provided for the principal offence under this Bill.	Retained
Offence Relating to Breach of Confidentiality	Retained

52.-(1) No person who is or has been the Data Protection Commissioner or a staff of the Commission or an agent of the Commission shall disclose information which- (a) has been obtained by, or provided to, the Commission in the course of, or for the purposes of, the discharging of the regulator's functions; (b) relates to an identified or identifiable Data Subject; and (c) is not available to the public from other sources at the time of the disclosure and has not previously been available to the public from other sources, unless the disclosure is made with lawful authority. (2) A person commits an offence who knowingly or recklessly discloses information in contravention of subsection (1) of this section and shall be liable upon conviction to a term of not less than 2 years imprisonment or a fine of not less than N10,000,000.00 or to both such term of imprisonment and fine.	
Order of Forfeiture of Assets 53.-(1) The Court may in addition to imposing sentence on any person convicted of an offence under this Bill, order that the convicted person forfeits to the Government of the Federal Republic of Nigeria- (a) any asset, money or property, whether tangible or intangible, traceable to proceeds of such offence; and (b) any computer, equipment, software, electronic device or any other device used or intended to be used to commit or to facilitate the commission of such offence; (2) where it is established that a convicted person has assets or properties in a foreign country, acquired as a result of such criminal activities for which he is convicted, such assets or properties, shall subject to any Treaty or arrangement with such foreign country, be forfeited to the Federal Government of Nigeria. (3) It is the responsibility of the Attorney-General of the Federation and Minister of Justice to ensure that the forfeited assets or properties are effectively transferred and vested in the Federal Government of Nigeria.	Retained
Order of Payment of Compensation or Restitution 54. -(1) In addition to any other penalty prescribed under this Bill, the Court shall order a data controller, data processor or person convicted of an offence under this Bill to make restitution to the victim of the offence. (2) an order of payment of compensation or restitution may be enforced by the victim or by the Commission on behalf of the victim in the same manner as a judgment in a civil action.	Retained
Part XIII - Records Obtained Under Data Subject's Rights Of Access Conditional Request for Personal Data Prohibited 55.-(1) A person who provides goods, facilities or services to the public shall not require a person to supply or produce a particular record as a condition for the provision of the goods, facilities or services to that person. (2) Subsection (1) does not apply where the imposition of the requirement is required for the identification of persons or authorized under an enactment; rule of law, valid commercial transaction or in the public interest.	Retained
Demand for health records prohibited 56.-(1). A person shall not be required to provide records which-	Retained

(a) consist of information related to the physical, mental health or mental condition of an Data Subject, or (b) has been made by or on behalf of a health professional in connection with the care of that Data Subject. (2) Subsection (1) does not apply where the imposition of the requirement is required or authorized under an enactment; rule of law, or in the public interest.	
Part XIV - Financial Provisions Funds of the Commission 57.-(1) The Commission shall establish and maintain a fund from which all expenditures incurred by the Commission shall be defrayed. (2) The Fund shall comprise funds derived from but not limited to the following sources- (a) such monies as may be appropriated to the Commission from time to time by the National Assembly; (b) gifts, loans, grants, aids, etc. ; (c) all other assets that may from time to time accrue to the Commission; and (d) Penalties and fines. (3) The provisions of any enactment relating to the taxation of companies or trust funds shall not apply to the Commission.	Retained
Borrowing Powers, Gifts, etc 58.-(1) The Commission may, in accordance with the general authority given by the Minister of Finance, borrow such sums of money as the Commission may require in the exercise of its functions under this Bill or its subsidiary legislation. (2) The Commission may accept gifts or grants of money or aids or other property from national, bilateral and multi-lateral organizations and upon such terms and conditions, if any, as may be agreed upon between the donor and the Commission provided that such gifts are not inconsistent with the objectives and functions of the Commission under this Bill.	Retained
59.-(1) The Commission shall in each financial year prepare and present to the National Assembly through the President for approval, a statement of estimated income and expenditure for the following financial year. (2) Notwithstanding the provisions of subsection (1), the Commission may also, in any financial year, submit supplementary or adjusted statements of estimated income and expenditure to the National Assembly through the President for approval. (3) Subject to subsections (1) and (2) of this section, the Commission shall apply the proceeds of the Commission's Fund- (a) to meet the administrative and operating costs of the Commission; (b) for the payment of salaries, wages, fees and other allowances, retiring benefits such as pensions and gratuities and, any other remunerations payable to the Commissioners and staff of the Commission; (c) for the purchase or acquisition of property or other equipment and other capital expenditure and for maintenance of any property acquired or vested in the Commission; (d) for purposes of investment; and	Retained

(e) for or in connection with all or any of the functions of the Commission under this Act or its subsidiary legislation.	
Financial Year and audit by the Commission 60. -(1) The financial year of the Commission shall start on 1st January of each year and end on 31st December of the same year. (2) The Commission shall keep proper records of its accounts in respect of each year and shall cause its accounts to be audited within 6 months from the end of each financial year by auditors whose appointment shall be approved by the Board and shall be subject to reappointment on annual basis provided that such auditors are on the list of auditors approved from time to time by the Auditor-General for the Federation.	Retained
Annual Reports 61. The Commission shall prepare and submit to the President, not later than 3 months after the end of its financial year, a report on the activities of the Commission for the preceding financial year and shall include therein the Commission's audited accounts for the year under review together with the auditor's report thereon.	Retained
PART XV - MISCELLANEOUS Procedure in respect of suits against the Commission 62. -(1) Notwithstanding anything contained in any other enactment or law, no suit against the Commission, or any employee of the Commission, for any act done in pursuance or execution of this Act, any law, or any public duty of the Commission, or in respect of an alleged neglect or default in the execution of this Act, such law, duty or authority, shall lie or be instituted in any court, unless it is commenced within three months next after the ceasing thereof. (2) No suit shall be commenced against the Commission before the expiration of a period of one month after written notice of intention to commence the suit shall have been served upon the Commission by the Intending plaintiff or his agent; and the notice shall clearly and explicitly state the- (a) course of action; (b) particulars of the claim; (c) name and place of abode of the intending plaintiff; and (d) relief he or she seeks. (3) Subject to the provisions of this Act, the provisions of the Public Officers Protection Act shall apply in relation to any suit instituted against an official or employee of the Commission.	Retained
Service of Documents 63. The notice pursuant to the provision of this Act or any other notice, summons, process, or other document required or authorized to be served upon the Commission under the provisions of this Act or any other law or enactment, may be served by delivering same to the Data Protection Commissioner of the Commission, or by sending it by registered post addressed to the Data Protection Commissioner at the head office of the Commission.	Retained
Restriction on execution against property of the Commission 64. No execution or attachment or process in the nature thereof shall be issued against the property of the Commission in respect of an action or suit against the Commission but the sums of money which by judgment of the court is awarded against the Commission shall be paid from the funds of the Commission.	Retained
Indemnity of Staff, Members, and Employees of the Commission	Retained

65. A Commissioner, member, agent, auditor or employee for the time being of the Commission shall be indemnified out of the assets of the Commission against any liability incurred in defending any proceeding whether civil or criminal, where any such proceeding is brought against him in his capacity as such staff member, agent, auditor or employee.	
International cooperation 66. The Commission shall perform the data protection functions that are necessary to give effect to any international obligations of the Federal Republic of Nigeria, subject to the powers vested in the Attorney General of the Federation.	Retained
Regulations, Guidelines and Review thereof 67. The Commission may when it deems necessary, review Guidelines or Regulations made under this Act that are in effect at the time of the review, and may in the process modify, vary or repeal any such Guidelines or Regulations- (a) which may no longer be relevant in the existing context of the Nigerian or universal System; (b) which may no longer be necessary in the national interest; (c) which may no longer be necessary to ensure the objects of this Act or its subsidiary legislation; or (d) for any other reason the Commission may consider necessary for giving full effect to the provisions of this Act and for its due administration.	Retained
Jurisdiction 68. The Federal High Court shall have exclusive jurisdiction over all matters, suits and cases howsoever arising out of or pursuant to or consequent upon this Act or its subsidiary legislation.	Retained
Power of Arrest, Search and Seizure 69.-(1) A law enforcement officer may apply ex-parte to a Judge in chambers for the issuance of a warrant for the purpose of obtaining electronic evidence in related crime investigation. (2) The Judge may issue a warrant authorizing a law enforcement officer to- (a) enter and search any premises or place if within those premises, place or conveyance- (i) an offence under this Act is being committed; (ii) there is evidence of the commission of an offence under this Act or other relevant law; or (iii) there is an urgent need to prevent the commission of an offence under this Act or other relevant law. (b) search any person or conveyance found on any premises or place which such authorized officers who are empowered to enter and search under paragraph (a) of this subsection; (c) stop, board and search any conveyance where there is evidence of the commission of an offence under this Bill; (d) seize, remove and detain anything which is, or contains evidence of the commission of an offence under this Bill; (e) use or cause to use a computer or any device to search any data contained in or available to any computer system or computer network; (f) use any technology to decode or decrypt any coded or encrypted data contained in a computer into readable text or comprehensible format;	Retained

(g) require any person having charge of or otherwise concerned with the operation of any computer or electronic device in connection with an offence under this Bill to produce such computer or electronic device. (3) The court shall issue a warrant under subsection (2) of this section where it is satisfied that- (a) the warrant is sought to prevent the commission of an offence under this Bill or to prevent the interference with investigative process under this Act; or (b) the warrant is for the purpose of investigating cybercrime, cyber security breach, computer related offences or obtaining electronic evidence; or (c) there are reasonable grounds for believing that the person or material on the premises or conveyance may be relevant to the cybercrime or computer related offences under investigation; or (d) the person named in the warrant is preparing to commit an offence under this Bill.	
Interpretation 70. In this Act- "Automated Data Subject decision making and profiling" means a decision based solely on automated processing, including profiling and shall only be processed pursuant to this Act; "Commission" means the Data Protection Commission, which is established pursuant to the provision of this Act; "consent of the Data Subject" means any freely given, specific (relating to such separate purpose) informed and unambiguous indication of the Data Subject's wishes by which he, by statement or by clear affirmative action, signifies agreement to the processing of Personal Data relating to him; "data Controller" means the natural or legal person, public authority, service, Commission or any other body which, alone or jointly with others, has decision-making power concerning determining the purposes and means of data processing, where a Data Controller also serves as a Data Processor, the provisions regarding the activities of a Data Controller under this Act shall apply; "data processing" means any operation or set of operations performed on Personal Data, such as- (a) collection, recording, organisation, structuring, storage or preservation; (b) adaption or alteration; (c) access, retrieval or consultation; (d) transmission, disclosure, sharing or making available; (e) restriction, erasure, or destruction of, or the carrying out of logical or arithmetical operations. Where automated processing is not used, "data processing" means an operation or set of operations performed upon Personal Data within a structured set of such data which are accessible or retrievable according to specific criteria; "Data Processor" means the natural or legal person, public authority, service, Commission or any other body which, alone or jointly with others processes Personal Data on behalf of the Data Controller; "Data Subject" means an identified or identifiable living natural person to whom	Retained

Personal Data relates; "identifiable Data Subject or identifiable natural person" means a natural person who can be identified directly or indirectly, in particular by reference to an identifier such as a name, identification number, online identifier, and includes 'singling-out' a natural person; "Personal Data" means any information relating to an identified or identifiable natural person (Data Subject); "Recipient" means a natural person or legal person or public authority, service, Commission or any other body to whom data is disclosed or made available; "Sensitive data" means - (a) Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership; (b) genetic data; (c) biometric data for the purpose of uniquely identifying a natural person; (d) data concerning health; (e) data concerning a natural person's sex life; (f) Personal Data relating to criminal offences, including criminal records; or (g) such other Personal Data that may from time to time be designated as sensitive data by Guidelines made by the Commission; The processing of any sensitive data shall be prohibited or allowed subject to appropriate safeguards pursuant to this Act; "third party" means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorized to process personal data	
Transitional provisions 71.-(1) A Data Controller incorporated or established after the commencement of this Act shall be required to register as a Data Controller within twenty days of the commencement of business. (2) A Data Controller in existence at the commencement of this Act shall be required to register as a Data Controller within three months after the commencement of this Act.	Retained
Savings Provision 72. Nothing in this Bill shall nullify or invalidate any provision of an Act of the National Assembly regarding safeguarding privacy of personal data.	Retained
Citation 73. This Bill may be cited as the Data Protection Bill, 2019.	Retained
Schedule [Section 8 (3)] Supplementary Provisions Relating To Proceedings Of The Commission 1. Subject to the provisions of this Bill and section 27 of the Interpretation Act, the Commission may make standing orders regulating the proceedings of the Commission and set up any committee thereof. 2. Every meeting of the Commission shall be presided over by the Data Protection	Retained

Commissioner/ Chief Executive Officer who shall preside as the Chairman. If the Chairman is unable to attend a particular meeting, the members present at the meeting shall elect one of their members to preside at the meeting.

3. The quorum at a meeting of the Commission shall consist of the Chairman (or in an appropriate case, the person presiding at the meeting pursuant to paragraph 2 of this Schedule and 4 other members.

4. Upon any special occasion, the Commission may co-opt any person to be member for as many meetings as may be necessary, and that person while so co-opted shall have all the rights and privileges of a member, except that he shall not be entitled to vote or count towards a quorum.

Committees

5.-(1) Subject to its standing orders, the Commission may appoint such number of standing and ad hoc committees as it thinks fit to consider and report on any matter with which the Commission is concerned.

(2) Every committee appointed under the provisions of sub-paragraph (1) of this paragraph shall be presided over by a member or Director of the Commission and shall be made up of such number of persons, as the Commission may determine in each case.

6. The decision of a committee shall be of no effect until it is confirmed by the Commission.

Miscellaneous

7. The fixing of the seal of the Commission shall be carried out by the Secretary of the Commission and authenticated by the signature of the Data Protection Commissioner/ Chief Executive Officer or such other Member or Director authorized generally or specifically by the Commission to act for that purpose.

8. Any contract or instrument which, if made by a person not being a body corporate, would not be required to be under seal, may be made or executed on behalf of the Commission by the Data Protection Commissioner/CEO or by any other Director or staff generally or specifically authorized by the Commission to act for that purpose.

9. Any document purporting to be a contract, an instrument or other document signed or sealed on behalf of the Commission shall be received in evidence and, unless the contrary is proved, be presumed, without further proof, to have been so signed and sealed.

10. The validity of a proceeding of the Commission or a committee thereof shall not be adversely affected-

- (a) by any vacancy in the membership of the Commission;
- (b) by any defect in the appointment of a member of the Commission, staff or committee; or
- (c) by reason that a person not entitled to do so took part in the proceeding.

11. A member of the Commission or any of its committee who has a personal interest in any contract or arrangement entered into or proposed to be

considered by the Commission or committee shall declare his interest and shall not vote on any question relating to the contract or arrangement.	
Explanatory Memorandum This Bill seeks to provide a legal and institutional framework for the regulation of personal data processing by private and public organizations in order to avoid the deleterious effect of unauthorized access to Data Subject data. It strikes a balance between Data Subject privacy concerns and the interest of security agencies and others in need of access to Data Subject data in the overriding public interest of state security, commerce and other lawful means. The Data Protection Commission established under the Bill will ensure effective administration and enforcement of the privacy principles enshrined in the Bill.	Retained

